Risk Assessment Check List

Information Security Policy

	Yes	No	In Progress
1. Information security policy document			
Does an Information security policy exist, which is approved by the management, published and communicated as appropriate to all employees?	☐	☐	☐
Does it state the management commitment and set out the organizational approach to managing information security?	☐	☐	☐
2. Review and Evaluation			
Does the Security policy have an owner, who is responsible for its maintenance and review according to a defined review process?	☐	☐	☐
Does the process ensure that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical structure?	☐	☐	☐

Organizational Security

Information security infrastructure

	Yes	No	In Progress
1. Allocation of information security responsibilities			
a. Are responsibilities for the protection of individual assets and for carrying out specific security processes clearly defined?	☐	☐	☐
2. Co-operation between organizations			
a. Are the appropriate contacts with law enforcement authorities, regulatory bodies, utility providers, information service providers and telecommunication operators maintained to ensure that appropriate action can be quickly taken and advice obtained, in the event of an incident?	☐	☐	☐
3. Independent review of information security			

	Yes	No	In Progress
a. Is the implementation of security policy reviewed independently on regular basis? This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	☐	☐	☐

Security of third party access

1. Identification of risks from third party

a.	Are risks from third party access identified and appropriate security controls implemented?	☐	☐	☐
b.	Are the types of accesses identified, classified and reasons for access justified?	☐	☐	☐
c.	Are security risks with third party contractors working onsite identified and appropriate controls implemented?	☐	☐	☐

2. Security requirements in third party contracts

a.	Is there a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards?	☐	☐	☐

Outsourcing

1. Security requirements in outsourcing contracts

a.	Are security requirements addressed in the contract with the third party, when the organization has outsourced the management and control of all or some of its information systems, networks and/ or desktop environments?	☐	☐	☐
	Does contract address how the legal requirements are to be met, how the security of the organization's assets are maintained and tested, and the right of audit, physical security issues and how the availability of the services is to be maintained in the event of disaster?	☐	☐	☐

Asset classification and control

Accountability of assets

	Yes	No	In Progress
1. Inventory of assets			
a. Is there a maintained inventory or register of the important assets associated with each information system?	☐	☐	☐

Information classification

1. Classification guidelines			
a. Is there an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected?	☐	☐	☐
2. Information labeling and handling			
a. Is there an appropriate set of procedures defined for information labeling and handling in accordance with the classification scheme adopted by the organization?	☐	☐	☐

Personnel security

Security in job definition and Resourcing

1. Including security in job responsibilities			
a. Are security roles and responsibilities as laid in Organization's information security policy documented where appropriate?	☐	☐	☐
Does this include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities?	☐	☐	☐
2. Confidentiality agreements			
a. Do employees sign Confidentiality or non-disclosure agreements as a part of their initial terms and conditions of the employment and annually thereafter?	☐	☐	☐
b. Does this agreement cover the security of the information processing facility and organization assets?	☐	☐	☐
3. Terms and conditions of employment			
a. Do the terms and conditions of the employment cover the employee's responsibility for	☐	☐	☐

	Yes	No	In Progress
information security? Where appropriate, these responsibilities might continue for a defined period after the end of the employment.			

User training

1. Information security education and training

a.	Do all employees of the organization and third party users (where relevant) receive appropriate Information Security training and regular updates in organizational policies and procedures?	☐	☐	☐

Responding to security/threat incidents

1. Reporting security/threat incidents

a.	Does a formal reporting procedure exist, to report security/threat incidents through appropriate management channels as quickly as possible?	☐	☐	☐

2. Reporting security weaknesses

a.	Does a formal reporting procedure or guideline exist for users, to report security weakness in, or threats to, systems or services?	☐	☐	☐

Physical and Environmental Security

Equipment Security

1. Equipment location protection

a.	Are items requiring special protection isolated to reduce the general level of protection required?	☐	☐	☐
b.	Are controls adopted to minimize risk from potential threats such as theft, fire, explosives, smoke, water, dist, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation and flood?	☐	☐	☐

2. Power Supplies

	Yes	No	In Progress
a. Is the equipment protected from power failures by using redundant power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator etc.?	☐	☐	☐

3. Equipment Maintenance

a. Is maintenance is carried out only by authorized personnel?	☐	☐	☐
b. Is the equipment is covered by insurance, and are the insurance requirements are satisfied?	☐	☐	☐

4. Securing of equipment offsite

a. Is any equipment usage outside an organization's premises for information processing has to be authorized by the management?	☐	☐	☐
b. Is the security provided for equipment while outside the premises equal to or more than the security provided inside the premises?	☐	☐	☐

5. Secure disposal or re-use of equipment

a. Are storage devices containing sensitive information either physically destroyed or securely over written?	☐	☐	☐

General Controls

1. Removal of property

a. Can equipment, information or software be taken offsite without appropriate authorization?	☐	☐	☐
b. Are spot checks or regular audits conducted to detect unauthorized removal of property?	☐	☐	☐
c. Are individuals aware of these types of spot checks or regular audits?	☐	☐	☐

Communications and Operations Management

Operational Procedure and responsibilities

1. Documented Operating procedures

a. Does the Security Policy identify any Operating procedures such as Back-up, Equipment maintenance etc.?	☐	☐	☐

	Yes	No	In Progress
2. Incident management procedures			
a. Does an Incident Management procedure exist to handle security/threat incidents?	☐	☐	☐
b. Does the procedure address the incident management responsibilities, orderly and quick response to security/threat incidents?	☐	☐	☐
c. Does the procedure address different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them?	☐	☐	☐
d. Are the audit trails and logs relating to the incidents are maintained and proactive action taken in a way that the incident doesn't reoccur?	☐	☐	☐
3. External facilities management			
a. Are any of the Information processing facilities managed by an external company or contractor (third party)?	☐	☐	☐
b. Are the risks associated with such management identified in advance, discussed with the third party and appropriate controls incorporated into the contract?	☐	☐	☐
c. Is necessary approval obtained from business and application owners?	☐	☐	☐

Media handling and Security

1. Management of removable computer media			
a. Does a procedure exist for management of removable computer media such as tapes, disks, cassettes, memory cards and reports?	☐	☐	☐

Exchange of Information and software

1. Information and software exchange agreement			
a. Is there any formal or informal agreement between the organizations for exchange of information and software?	☐	☐	☐

	Yes	No	In Progress
b. Does the agreement address the security issues based on the sensitivity of the business information involved?	☐	☐	☐
2. Other forms of information exchange			
a. Are there are any policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities?	☐	☐	☐

Access Control

Business Requirements for Access Control

1. Access Control Policy			
a. Are the business requirements for access control have been defined and documented.	☐	☐	☐
b. Does the Access control policy address the rules and rights for each user or a group of users?	☐	☐	☐
c. Are the users and service providers given a clear statement of the business requirement to be met by access controls?			

Mobile computing and telecommuting

1. Mobile computing			
a. Has a formal policy been adopted that takes into account the risks of working with computing facilities such as notebooks, palmpilots etc., especially in unprotected environments?	☐	☐	☐
b. Was training arranged for staff that use mobile computing facilities to raise their awareness on the additional risks resulting from this way of working and controls that need to be implemented to mitigate the risks?	☐	☐	☐
2. Telecommuting			
a. Are there any policies, procedures and/ or standards to control telecommuting activities, this should be consistent with organization's security policy?	☐	☐	☐

	Yes	No	In Progress
b. Is suitable protection of telecommuting site in place against threats such as theft of equipment, unauthorized disclosure of information etc.?	☐	☐	☐

Business Continuity Management

Aspects of Business Continuity Management

	Yes	No	In Progress
1. Business continuity management process			
a. Is there a managed process in place for developing and maintaining business continuity throughout the organization? This might include Organization wide Business continuity plan, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.,	☐	☐	☐
2. Business continuity and impact analysis			
a. Are events that could cause interruptions to business process were identified? Example: equipment failure, flood and fire.	☐	☐	☐
b. Was a risk assessment was conducted to determine impact of such interruptions?	☐	☐	☐
c. Was a strategy plan was developed based on the risk assessment results to determine an overall approach to business continuity?	☐	☐	☐
3. Writing and implementing continuity plan			
a. Were plans developed to restore business operations within the required time frame following an interruption or failure to business process?	☐	☐	☐
b. Is the plan regularly tested and updated?	☐	☐	☐
4. Business continuity planning framework			
a. Is there a single framework of Business continuity plan?	☐	☐	☐
b. Is this framework maintained to ensure that all plans are consistent and identify priorities for	☐	☐	☐

		Yes	No	In Progress
	testing and maintenance?			
c.	Does this identify conditions for activation and individuals responsible for executing each component of the plan?	☐	☐	☐

5. Testing, maintaining and re-assessing business continuity plan

a.	Are the Business continuity plans tested regularly to ensure that they are up to date and effective?	☐	☐	☐
b.	Are the Business continuity plans maintained by regular reviews and updates to ensure their continuing effectiveness?	☐	☐	☐
c.	Are procedures included within the organizations change management program to ensure that Business continuity matters are appropriately addressed?	☐	☐	☐